

# **ZKAccess4.5 Quick Use Guide**

---

Version: V 1.0

Software Version: For ZKAccess 4.5.8 or above Version

Date: July, 2011

The guide is the simplified version of the User Manual. It is used for the user to grasp the operation of the system as soon as possible. For more details, please consult the User Manual.



# Table of Contents

<b>1. Overview of System Modules.....</b>	<b>2</b>
<b>2. Simplified Process for Use.....</b>	<b>4</b>
2.1 Log in the System .....	4
2.2 Device Management .....	4
2.3 Personnel Management.....	7
2.4 Access Time Zone.....	9
2.5 Access Control Holidays.....	11
2.6 Door Setting.....	12
2.7 Setting of Access Levels.....	13
2.8 Setting of Personnel Access Levels .....	14
2.9 Real-time Monitoring and Real-time Events .....	15
2.10 Report .....	16
<b>3. Database Management .....</b>	<b>17</b>
3.1 Setting of Database Backup Path.....	17
3.2 Back up Database .....	17
3.3 Restore Database .....	17

# 1. Overview of System Modules

**Personnel management:** Personnel management mainly contains the following three parts: [Department], [Personnel] and [Issue Card]. After personnel are categorized according to departments, privilege can be granted to the personnel of a department in batches in [Personnel Access Levels] conveniently.

**Device management:** It is mainly used for adding, searching and deleting access control panel. The user can divide the device by using the areas reasonably. In this way the device can be filtered as per areas in monitoring, and the user can also set the administration users to manage the device in some areas in [System Setting] - [User].

**Door setting:** When the user adds an access control panel in the system, the system will add the doors of corresponding number according to the parameters of the access control panel automatically, and the user need not to add them manually. The user needs to modify the parameters of each door according to actual needs.

**Access time zone:** After an access time zone is newly added, the user can select the time zone when an access level is newly added in [Access Levels]. At this time, the time zone will be used as the door opening time for the personnel within the scope of control privilege. Each time zone contains days from Sunday to Saturday and three holiday categories and each corresponding day contains three intervals.

**Access control holidays:** After holidays are newly added and types of holidays are set, the user can set the interval for a specific type of holiday in a time zone.

**Access Level:** The access level is the core part of the system, and it is the combination of doors with access privileges containing and within access control intervals. After the combination is set up, apart from allocating privileges in batches in [Personnel Access Levels], access privilege can be allocated to individuals in [Personnel] - [Personnel] .

**Personnel Access Levels Setting:** Allocate the established access privileges to the personnel. In short, it is to set who has the access privilege to open which doors in a time zone (containing several intervals).

**Real-time monitoring:** Current user in the monitoring system has the privilege to manage and view the status of doors and real-time events contained in the access control panel, including normal and abnormal events (alarm events included).

**Report:** The report contains records of real-time events and the setting of personnel access privileges. Historical records required by the users can be viewed and output through the report.

**System setting:** Administration users with different roles can be allocated, and a role refers to the operation privilege of the user for the current system (nothing to do with access level). And the user can perform backup and initialization of the database in database management. [Service Controller] on the server can only be used for restoration of database (click [Start] - [Program] - [ZKAccess4.5 Access Management System] - [Service Controller] on the server to open it).

**Note:** In the operation system of Windows Vista or above, right click the [Service Controller] icon and select [Open It as the Administrator] to realize the function.

**Data communication center:** After the user operates in the system (including add, edit, delete or other functional settings), just maintain normal communication between the server and the equipment, and the system will synchronize relevant information to the device automatically. In normal conditions, the user does not need to synchronize the data manually. In [Device Monitoring], the user can see if the device communicates normally in a visual way and see the progress of data synchronization. [Synchronize All Data] in [Device] - [Device] can only be used in special circumstances. And during the operation, the system will synchronize the data in the target device with the current system.

## 2. Simplified Process for Use

### 2.1 Log in the System

The default access port for the system is 80. If the IP address of the server is 192.168.1.8, any client with network connection can access the system directly through <http://192.168.1.8:80> (or <http://192.168.1.8>) in the browser. If this URL is not accessible in the client, please ensure the 80 port is not disabled by the firewall of the server. If it is disabled, please add the 80 port to the exception (recommended), or close the firewall (not recommended).

Enter the assigned user name and the password (the initial user name and password are both “admin”), or click [Fingerprint Login], and then press the administrator fingerprint on the fingerprint sensor (need to install the fingerprint sensor driver first) to log in the system. After logging in the system with the default account number, it is recommended to modify the initial password and ensure it is safety.

After logging in the system, enter [My Work Panel] interface.

### 2.2 Device Management

Click [Device] on the top left corner of [My Work Panel] directly to enter device management module.

1. Click the menu [Area Setting] and modify the area added in the initialization of the system. E.g. fill in the name, company and so on.

To modify the default area, there's no need to select the upper area.

The user can add other areas according to their needs, and the relationship between areas needs only to be set in accordance with the structure of the company, enterprise or institution at setting.

2. Click [Device] menu. Two type of device supported in the system, access control panel and network video recorder.

## 2. Simplified Process for Use

(1) For access control panel, there two ways for adding device in the software. First, the newly added way will be illustrated.

Click [Add] button and select to add the access control panel, the following interface appears (such as TCP/IP mode):

Current Window: Device -> Device-> Add

The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.

**Step 2: Add Device Information( Access Control Panel )**

\*Device Name:

\*Communication Mode: ☒ TCP/IP ☐ RS485

\*IP Address:

\*IP Port No. :

Communication Password:

Access Control Panel Type:

Auto Synchronize Device Time: ☒

\*Area:

Clear Data in the Device when Adding: ☒

The user shall fill in device name, communication parameters (such as IP address, IP port number or 485 address, serial port number, baud rate), select a communication mode, type of access control panel and the area its belongs to. The device name shall be as simply and clear as possible.

The communication password shall be filled in for adding the device whose communication password has been set. The communication password for all new devices is blank by default.

After adding device, to prevent the malicious access to the system, the user can use [Modify Communication Password] in [Access Control] - [Door Setting] - [Door Management] to set the communication password.

**Switch to two-door and two-way mode.** It is only used when four-door and one-way access control panel is used as two-door and two-way access control panel. The user needs not to tick it in other circumstances. It is suggested that the user tick

auto synchronize device time to ensure the time on the access control panel is consistent with that on the server.

**Clear Data in the Device when Adding.** By default it is ticked, namely, it will clear the data in the device after you have added a device to the system. All access levels will be cleared, but events logs will be left. If you add the device just for demonstration and testing of the system, don't tick it.

Click [OK] button. If a dialog box appears, go on clicking [OK], and the system will attempt to connect the device.

If the system prompts that connection succeeds, click [OK], and the system starts to add device.

At this time, the newly device can be found on the devices list.

Another way to add the device is by [Search Access Control Panel] (only access control panel in Ethernet is supported temporarily). The result after search is as follows:

Current Window: Device -> Device -> Search Access Control Panels

☒ Search for the access control panels on the TCP/IP network.

☒ Search result

The total number of access control panels found now is:53

IP Address	MAC Address	Subnet Mask	Gateway	Serial Number	Device Type	Operation
192.168.1.201	00:17:61:7F:1E:40	255.255.255.0	192.168.1.201	5000031100001		This device has been added.
192.168.8.46	00:17:61:7F:19:AC	255.255.255.0	192.168.8.46	4154245424		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.8.122	00:17:61:18:00:E2			201008260058	ACP	<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.8.123	00:17:61:18:00:D9			20100501999	ACP	<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.8.133	00:17:61:7F:10:90	255.255.255.0	192.168.8.133	47474744444478		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.8.190	00:17:61:7F:10:CF	255.255.255.0	192.168.8.254	20100501999	ACP	<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.107	00:17:61:7F:0D:AD	255.255.255.0	192.168.200.254	565632650001113		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.108	00:17:61:7F:0D:BC	255.255.255.0	192.168.200.108	565632650003		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.110	00:17:61:7F:2D:A1	255.255.255.0	192.168.200.254	20110304105048		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.111	00:17:61:7F:0F:65	255.255.255.0	192.168.200.111	47474874874845		<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.113	00:17:61:7F:2C:F5	255.255.255.0	192.168.200.113	1761808093	ACP	<a href="#">Modify IP Address</a> <a href="#">Add Device</a>
192.168.200.218	00:17:61:7F:2C:F5	255.255.255.0	192.168.200.254	1761808093	ACP	<a href="#">Modify IP Address</a> <a href="#">Add Device</a>



## 2. Simplified Process for Use

Click [Add Device] in [Operation] column to pop up a prompt box to modify device name, and it is an IP address by default in the system, and the user can modify it to a concise name according to your needs. After clicking [OK], the device is added successfully.

(2) In new device adding interface, select to add a network video recorder and click [Next], and the following interface appears;

Current Window: Device -> Device-> Add

The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.

Step 2: Add Device Information( Network Video Recorder )

\*Device Name:

\*IP Address:

\*IP Port No. : 8000

\*Username:


Communication Password:

\*Area:

Save and Continue OK Cancel

User need to fill the following information, such as IP address, IP port, User name and etc. After that, clock [OK] to finish the new device adding.

The system supports Hikvision network video recorder only by now. For more detail, please refer to the software user manual.

 **Note:** This feature is only available for the professional version of software, if you need to use, please contact with our pre-sales or technical support.

## 2.3 Personnel Management

Enter the module [Personnel] from the menu on the left top corner.

Click [Department] to enter department management interface, and modify the default department name into actual name (such as company name or name of enterprise or institution). Then the user can set up a directory structure of departments with a clear hierarchical level according to actual needs.


The user can use the categorization of personnel by departments according to actual needs, for instance, they can categorize the personnel as class, dormitory and department of the company.

Click [Personnel] to enter personnel management. Click [Add] to show the following interface:

Current Window: Personnel -> Personnel-> Add

Personnel information is the system's basic information, so No. and department are required items.  
an access control panel only supports 6-digit passwords. If a password exceeds the specified length, the system will truncate it automatically!

### Personnel Profile

*Personnel No.:	<input type="text"/>	<input type="button" value="Check"/>	Nationality:	<input type="text"/>	 Upload Personal Photo (Optimal Size 120×140 Pixel) <input type="button" value="Browse"/>
First Name:	<input type="text"/>		City:	<input type="text"/>	
Last Name:	<input type="text"/>		Postal Code:	<input type="text"/>	
Gender:	<input type="text"/>		Office Telephone:	<input type="text"/>	
Card Number:	<input type="text"/>		Home Telephone:	<input type="text"/>	
Password:	<input type="text"/>		Mobile Phone:	<input type="text"/>	
*Department:	<input type="text"/>		Ethnic:	<input type="text"/>	
Social Security Number:	<input type="text"/>		Birthday:	<input type="text"/>	
Education:	<input type="text"/>		Job Title:	<input type="text"/>	
Employment Date:	<input type="text" value="2011-06-08"/>		Email:	<input type="text"/>	
Employment Type:	<input type="text"/>		Origin:	<input type="text"/>	
Type:	<input type="text"/>		Work Address:	<input type="text"/>	
Political Status:	<input type="text"/>		Home Address:	<input type="text"/>	

### Access Control Settings

Access Levels: ☐ test

Set Valid Time: ☐

Multi-Card Opening Personnel Groups:

The upper part is the basic information of the personnel. The personnel numbers can be work card number or student number, but the number can not be repeated. The department is compulsory. Other information can be filled optionally by the user according to their needs.

If the user needs to issue a card for the newly added personnel, they can input the card number directly in the text box behind the card number (or read the card number through card reader).

The lower part mainly involves setting of access privileges. If existing access level shall be allocated for the user, select it directly here (If there is no access level added in the system, you can see the prompt of red words in the above figure). Setting of effective time is applicable for visitors and other occasions that the personnel have the privilege to open the door. Multi-card opening personnel group is used for multi-card door opening function. If this function is not used, just leave it blank.

**If cards are to be issued in batches to those enrolled personnel without cards, the function of [Issue Cards in Batches] can be used. Refer to the User Manual for specific directions.**



**Notes:** Two modes for setting of personnel access levels are available in the system.

The first is to add personnel (without setting access level) in [Personnel] - [Personnel], add an access level in [Access Control] - [Access Levels] and set personnel access levels in [Access Control] - [Personnel Access Levels].

The second is to add an access level in [Access Control] - [Access levels] and select an access level directly when adding or editing personnel in [Personnel] - [Personnel].

The demonstration in the later part of the document is the first mode.

### 2.4 Access Time Zone

The time zone of [24-hour Accessible] is added by default in the system. In this time zone, there is a time zone for every day, namely it is accessible for 24 hours.

Each time zone contains days from Sunday to Saturday and three holiday types and each corresponding day contains three intervals.

Example 1: To set [Effective Time Zone] of a Door, the effective time within this time zone from Monday to Friday is 08:00-12:00,13:00-18:00,19:00-21:00, that on holidays as per [Holiday Type 1] is 08: 00-22:00, that on holidays as per [Holiday Type 2] is 12:00-23:00, and there is no holiday with type of holidays set as per [Holiday Type 3] .

 Current Window: Access Control System -> Time zones-> Add

The End Time must always be greater than the Start Time, except that the start and end time are both '00:00'.

\*Time Zone Name:

Remarks:

Date	Time	Interval 1		Interval 2		Interval 3	
		Start Time	End Time	Start Time	End Time	Start Time	End Time
Monday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Tuesday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Wednesday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Thursday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Friday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Saturday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Sunday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 1		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 2		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 3		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00

 Save and New  OK  Cancel

The following points shall be noted for setting:

1. Three intervals are available for each day in the system. If the user only uses one or two of them, he can just keep the default value for the remaining two or one intervals as (00:00-00:00).
2. If the [Holiday Type 3] has not being set, just keep the default value (00:00-00:00) for three intervals within the time zone.
3. There shall not be any overlapping time between the three intervals.

After the time zone is set, set it as the effective time zone of a door.

### 2.5 Access Control Holidays

If access control holidays are not required, please skip this part directly, and keep the default value (00:00-00:00) unchanged for the corresponding interval in the access time zone.

To add access control holidays, the user needs to select a holiday type from the three holiday types available in the system. Apart from categorization of holidays, the function of holiday types are mainly used for the day that is set as a holiday, when the system select the interval of the holidays from the selected time zones as the effective time by priority (including effective door events and effective door opening time for personnel), namely, when the system select intervals from the time zones, priority level of holiday types 1, 2 and 3 is higher that intervals from Sunday to Saturday.


Click [Add] to show the following interface:


Current Window: Access Control System -> Holidays-> Add

Each holiday type cannot contain more than 32 holidays. A holiday cannot last more than 365 days.  
If a holiday lasts only one day, set its end date the same as the start date.  
Recurring means the dates of a holiday will not change in every year.

\*Name:




\*Type:

\*Start Date:  

\*End Date:  

\*Recurring:

Remarks:

 Save and New  OK  Cancel

The legal holiday of International Labor Day is added here. After combining it with [Time Zones Demo] in the above example, when the time is between starting date and ending date, because the holiday type of [Labor Day] is [Holiday Type 1], when the [Time Zones Demo] is used for the door of effective time zone, and it is effective from 8: 00 to 22: 00, and the door is forbidden at other time.

Access holidays in a broader sense contain other holidays requiring special treatment apart from legal holidays, such as the circumstance that door shall be open as usual at weekends due to adjustment of rest. The user needs only to set these special dates as the holidays of a holiday type in the system.



#### Notes:

1. Starting time and ending time of the set holidays can not be over a year.
2. The number of holidays contained in each holiday type can not exceed 32.

## 2.6 Door Setting

After adding device in [Device], enter [Access Control], and the newly added information for control panel and corresponding list of doors can be seen in [Door Setting] - [Door Management]:

Current Window: Access Control System -> Door Configuration -> Door Management

Search: Device Name: Access Control Panel Type: Door Name: Search Advanced Clear

Modify in address More... Total 3 Entry/1 Page 1/1

Device name	Communication method	Ip address	Serial port no.	485 address	Status	Enable	Device model	User quantity	Fingerprint quantity	Related operation
test2	TCP/IP	111.111.111.111								Edit
192.168.200.123	TCP/IP	192.168.200.123								Edit

Door number	Door name	Door active time range	First-Card Normal Open	Multi-Card Open	Related operation
1	192.168.200.123-1	24-Hour Accessible	Quantity Set: 0   Set	Quantity Set: 0   Set	Edit
2	192.168.200.123-2	24-Hour Accessible	Quantity Set: 0   Set	Quantity Set: 0   Set	Edit
3	192.168.200.123-3	24-Hour Accessible	Quantity Set: 0   Set	Quantity Set: 0   Set	Edit
4	192.168.200.123-4	24-Hour Accessible	Quantity Set: 0   Set	Quantity Set: 0   Set	Edit

192.168.200.123-4 TCP/IP 192.168.200.123-4 Edit

Click [Edit] in relevant operations and set door parameters for the control panel as shown in the following figure:

## 2. Simplified Process for Use

Current Window: Access Control System -> Door -> Details

This door can be enabled only when the door Active Time Zone has been set. If the door sensor type is selected as "None", the current status of the door cannot be detected during real-time monitoring. The 'Apply this setting to all the doors of current access control panel!' will only apply to the doors which has been allocated to the current users authorization settings. [Log Entries](#)

\*Device Name: 192.168.200.123

\*Door Number: 1

\*Door Name: 192.168.200.123-1

\*Door Active Time Zone: 24-Hour Accessible

Normal Open Time Zone:

\*Lock Drive Duration: 5 (10-254)

\*Punch Interval: 2 (10-10)

\*Door Sensor Type: None

\*Verify Mode: Card or Fingerprint

Duress Password: (max 8-digit integer)

Emergency Password: (max 8-digit integer)

Apply this settings to all the doors of current access control panel: ☐

Apply this settings to all the doors of all access control panels: ☐

OK Cancel

Door name is the combination of device name and door number by default and it can be modified by the user.

Door sensor type can be selected according to actual needs of the user. The other parameters can be filled according to your needs and the default value can be used if there's no special need.

The two check boxes on the bottom are used for the user to apply the current door setting to other doors and prevent from repeated operations of the same setting.

### Notes:

If the user needs to use the functions of normal opening with first card, opening with multiple cards, anti-pass back, interlock and linkage, they can enter from the relevant buttons on the page of [Access] - [Door Setting]. Please refer to the User Manual for detailed setting methods, and there will not be detailed description on the current document.

## 2.7 Setting of Access Levels

Before allocating access privilege to personnel, add the access levels allocated for use of specific groups, mainly consisting of the combination of access time zone and door, namely which time zone is set to open which doors.

Enter [Access Control] - [Access Levels], and click [Add] to show the edit interface.

The user needs only to select time zone to be set and the door to be controlled.



**Notes:**

The access time zone selected here is preset in [Access Control] - [Access Time Zone] , which means that the time zone selected here can be the same as the effective time zone for doors and normally open time zone for doors (also includes access time zone selected for normal opening with first card) selected in [Door Setting] - [Door Management] above. For instance, if the effective time zone for the control panel in the current system and door opening time for all people to be allocated are all day long, just select the time zone [24 hours accessible] by default in the system. If the user needs to use special time zone in the access levels or other occasions to use access time zones, the user need to add specific access time zone in [Access Time Zone].

## 2.8 Setting of Personnel Access Levels

Enter [Access Control] - [Personnel Access Levels] - [Display with Access Levels] , click [Add Personnel] button to add personnel to the currently selected access level, and view and delete the personnel existing in the current access level.

When the user is switched to [Display as Personnel], after the user clicks a person on the left side, the access level for the person on the left side can be seen directly. Perform the operation of [Add Access Level] to add persons to the group with more access privileges and perform [Delete Access Level] to delete persons on the left side from the specific access level.



**Notes:** The system can meet needs of allocation of access privileges in batches or separately. When the user is performing the operation, he can use the function of search in the system to find out the required access level or personnel to reach accurate and rapid allocation of privileges.





### 2.9 Real-time Monitoring and Real-time Events

Enter [Access Control] - [Real-time Monitoring] - [Monitor all] as shown in the following figure:

Current Window: Access Control System -> Real-Time Monitoring -> Monitor All

**Door Status Monitoring**

Area:  Access Control Panel:  Door:

 inbi...  inbi...

**Events Monitoring** Alarm Events Detected

Time	Device	Event point	Event Description	Card Number	No.(Name)	In/Out Status	Verify Mode
2010-03-07 09:53:51	inbio	inbio-1	Duress Password Open	36656656	645	In	Only Card

The system provides monitoring of door status and that of real-time events. The user can change the options in the drop-down boxes in Area, Control Panel and Door to narrow or enlarge the monitoring scope. The default setting in the system is to monitor all the doors under the control panel that the current user has the privilege to view.

When the user switches to [Alarm Event], the system will only monitor the alarm events generated after the current time.




#### Notes:

1. Please refer to real-time monitoring part in the User Manual for all real-time events and their detailed descriptions.
2. Remote door opening and closing are emergent door opening and closing operations and they are not restricted by effective time zones of doors, namely, the door can be opened with this operation at any appropriate time. Make sure to operate

with caution. When a super administrator is allocating a new user ([System Setting] - [User]), to prevent other users from faulty operations, do not allocate the privilege in [Access Control] - [Real-time Monitoring] to new users.

User can use the [Electro-Map] function to view the current door state. After setting the video linkage function in the system, if the real-time linkage event happens, the preview interface will pop up in the real-time monitor interface.

 **Note:** The Electro-Map and video linkage functions are only available for the professional version of software, if you need to use, please contact with our pre-sales or technical support.

## 2.10 Report

After entering the report of [Access Control], the user can view [All Access Control Events] and [Personnel Access Levels] in accordance with their needs.

If the user wants to view [Access Control Exception Events], they can find out relevant records rapidly using search function.

Current Window: Access Control System -> Reports -> All Access Control Events

**Search**  
Time:   
Device:   
Verify Mode:

Personnel No.:   
Door Event Point:   
In/Out Status:

Card Number:   
Auxiliary Input Point:   
Event Description:

**All Events**

Total 993 Entry/97 Page

Time	Personnel no./Name	Card number	Device	Door event point	Auxiliary input point/Auxiliary output point	Verify mode	In/Out status	Event description
2011-03-29 19:16:34	0000000645 zy	--	192.168.200.123	192.168.200.123-2	None	None	Card or Fingerprint: In	Normal Fingerprint
2011-03-29 19:16:25	0000000645 zy	--	192.168.200.123	192.168.200.123-2	None	None	Card or Fingerprint: Out	Normal Fingerprint
2011-03-29 19:15:56	0000000645 zy	--	192.168.200.123	192.168.200.123-1	None	None	Card or Fingerprint: Out	Normal Fingerprint
2011-03-29 19:06:42	--	--	192.168.200.123	192.168.200.123-1	None	None	Others	Remote Operation
2011-03-29 19:05:00	0000000645 zy	--	192.168.200.123	192.168.200.123-1	None	None	Card or Fingerprint: Out	Access Denial
2011-03-29 16:41:33	--	--	inbio	inbio-1	None	None	Others	Remote Operation

### 3. Database Management

To prevent from damage and loss of data in database server caused by objective factors, it is recommended that the user use backup and restoration function in the system to manage the data in the system. The simple operations for backup and restoration of database is as follows:

#### 3.1 Setting of Database Backup Path

In software installation process, or the user needs to use [Service Controller] - [Set Database Backup Path] to configure database backup path on the server.

#### 3.2 Back up Database

1. Select [Immediate Backup] the system will start backing up the database. When the value in the column of “Whether backup successful” is changed from “Processing” to “Yes”, backup of database succeeds, and if it is changed to “No”, the backup fails.



**Notes:** It is recommended that the user backup the data after setting up personnel information, device information and setting part of access privileges. The system does not support backup of Oracle database temporarily.

2. After the system starts normal operations, the user can select [Scheduled Backup] for regular backup to prevent data losing.

#### 3.3 Restore Database

When the user needs to restore the database files that have been backed up, they need to find the backup files to be restored under the backup directory set before in [Service Controller] - [Restore Database] on the server and click [Restore] button.



**Notes:**

1. Do not close any command window popping up in the restoration process of the database.

Backup of the database can be operated at any client (browser) by the user with the privilege to back up the database. The setting of database backup path and restoration of database shall be operated at [Service Controller] on the server.

2. After the database backup path is set on the server, it is recommended that the user do not set up several planned backups at the same server, which will increase load of the server.

3. In case of failure of backup and restoration please refer to directions in [Service Controller] and [System setting] in the User Manual and relevant part in FAQ.